Listing of Claims:

Claim 1 (currently amended): A method performed by a hub for bypassing an access blocking apparatus and thereby ~~for~~ enabling a first device to allow communications from a second device wherein the first device is on a local network and the second device is external to the local network, the local network including ~~separated from the second device by~~ the access blocking apparatus that connects the local network to external networks and that separates the first and second devices, said method comprising:

terminating a virtual pipe from the first device,

assigning an IP address to the first device and associating this IP address with the virtual pipe,

receiving communications originated by the second device and addressed to said IP address,

routing the communications addressed to said IP address to the virtual pipe, and

tunneling the communications over the virtual pipe to the first device thereby bypassing the access blocking apparatus.

Claim 2 (original): The method of claim 1 further comprising the steps of:

receiving second communications originated by the first device through the virtual pipe, and

routing the second communications from the first device to the second device.

Claim 3 (original): The method of claim 1 further comprising the step of:

encrypting the communications prior to tunneling the communications over the virtual pipe.

Claim 4 (original): The method of claim 1 further comprising the steps of:

receiving a plurality of communications originated by a plurality of second devices and addressed to the IP address,

routing the plurality of communications addressed to the IP address to the virtual pipe, and

tunneling the plurality of communications over the virtual pipe to the first device.

Claim 5 (original): The method of claim 1 further comprising the steps of:

establishing an access control list to control access to the first device, and

based on the access control list, routing the communications from the second device to the first device only if the second device has permission to access the first device.

Claim 6 (original): The method of claim 1 further comprising the steps of:

terminating a second virtual pipe from the second device,

assigning a second IP address to the second device, and

receiving the communications from the second device through the second virtual pipe.

Claim 7 (original): The method of claim 6 wherein the IP addresses assigned to the first and second devices are private IP addresses.

Claim 8 (currently amended): A system for bypassing an access blocking apparatus and thereby ~~for~~ enabling communications between a first device and a second device wherein ~~said~~ the first device is on a local network and the second device is external to the local network, the local network including ~~separated from said second device by~~ the access blocking apparatus that connects the local network to external networks and that separates the first and second devices, said system comprising:

a secure hub, and

a virtual pipe between the first device and said secure hub,

said secure hub including a pool of available IP addresses from which an IP address can be assigned to the first device, and further comprising means for associating the assigned IP address with the virtual pipe, means for routing communications from the second device and addressed to the first device to the virtual pipe, and means for tunneling said communications over the virtual pipe to the first device thereby bypassing the access blocking apparatus.

Claim 9 (original): The system of claim 8 wherein said means for tunneling tunnels second communications over the virtual pipe from the first device, and wherein said means for routing routes the second communications to the second device.

Claim 10 (original): The system of claim 8 further comprising:

a virtual pipe between the second device and said secure hub, and wherein said means for associating associates a second IP address from the pool of available IP addresses with the

second virtual pipe, and wherein said means for tunneling tunnels said communications from the second device through the second virtual pipe.

Claim 11 (original): The system of claim 8 further comprising:

an access control list to control access to the first device, and wherein, based on the access control list, said means for routing the communications from the second device to the first device routes the communications only if the second device has permission to access the first device.

Claim 12 (currently amended): A system for enabling communication from a second communication device that is external to a local network ~~to a first communication device~~ through ~~the~~ a public network and bypassing a security access blocking apparatus ~~from a second communication device~~ to a first communication device on the local network, wherein said security access blocking apparatus provides the first communication device access to the public network and separates the first and second communication devices ~~being separated by at least one security access blocking apparatus~~, said system comprising

a secure hub having routing and switching functionality and pipe termination functionality and having interfaces to said public network, and

means for creating a virtual pipe between said secure hub and said first communication device for tunneling communication and bypassing said security access blocking apparatus,

said secure hub further including means for assigning an IP address to said first communication device and associating said IP address with said virtual pipe.

Claim 13 (original): The system of claim 12 further including means for establishing said communication from said second communication device through said public network to said secure hub.

Claim 14 (original): The system of claim 13 wherein said means for establishing said communication from said second communication device includes means for defining a second virtual pipe.

Claim 15 (original): The system of claim 12 wherein said secure hub includes means for defining an access control list, said routing and switching functionality routing said

A1

communication from said second communication device to said virtual pipe only if such access is permitted by said access control list.

Poier improves security and in general, provides any benefit at all. With respect to Murakawa alone, again these teachings fail to anticipate or obviate claim 1.

Specifically, Poier teaches a method whereby a centralized server facilitates the establishment of VPN (virtual private network) connections between nodes for communications over a public network. (Poier, paragraphs 41-43). However, Poier fails to teach or suggest that these nodes use this centralized server to bypass access blocking apparatus and enable communications as claim 1 recites. According to Poier, nodes desiring to communicate over a VPN first establish a secure connection to the centralized server. The server then delivers configuration information to the nodes in order for the nodes to establish and communicate over the VPN. (Poier, paragraph 43). Accordingly, although there are secure connections between two nodes and the centralized server, there is also a VPN between the nodes, which VPN does not traverse the centralized server and is used by the nodes to communicate. In particular, Poier notes that the server "is used for initial provisioning of the [VPN] and to transfer ... configuration information [to nodes] for the provisioning of the [VPN]. [The] VPN is established between the sets of nodes." (Poier, paragraph 48). Accordingly, Poier's nodes do not use the centralized server to bypass access blocking apparatus and enable communications, as claim 1 recites.

Applicants further note the Examiner's reference to Poier, paragraph 51, where Poier describes the situation where two nodes are separated by a device such as a NAT and wish to establish an end-to-end VPN through the NAT. Again, contrary to claim 1, Poier here is not concerned with bypassing the NAT, but rather, overcoming the specific issue that NATs tend to prevent nodes from establishing secure VPNs. (Poier, paragraph 12). The centralized server here is not the node of claim 1 because the server only plays the role of configuring the nodes to correctly establish the VPN but does not play a role in the actual transfer of data to bypass the NAT. (Poier, paragraphs 50-51). In particular, note that the NAT functionality is not being bypassed here. The NAT actually manipulates packets as they traverse the NAT (Poier, paragraph 53), implying that the NAT is configured to allow nodes to communicate, the essential problem applicants' invention as recited by claim 1 overcomes.

Applicants also note that the Examiner seems to indicate that Poier's NAT is the node of claim 1. Again, applicants respectfully disagree because the NAT does not terminate a virtual pipe and, again, the NAT functionality is not being bypassed here as just described.

The Examiner also makes reference to Poier, paragraph 49, where Poier describes the situation where a gateway, such as gateway 24 in Figure 4, controls access to several nodes behind the gateway, such as nodes 25. Here, one of the nodes 25 and a node in front of the gateway (i.e., a node in the external network), such as node 12b, wish to establish secure